WHAT IS CLAIMED IS:

1. A firewall system for preventing non-requested packets coming from a public network from reaching network elements connected thereto, said firewall system comprising:

a front-end server having internal and external interfaces; said front-end server external interface being attached to the public network; said front-end server being configured to drop non-requested incoming packets from the public network; said non-requested packets including signed packets and unsigned packets; and

a back-end server having internal and external interfaces; said back-end internal interface being attached to the network elements and to said front end internal interface via said back-end external interface; said back-end server being so configured as to gather packets requested by the network elements from the public network, and signed packets from the front-end server; said back-end server being configured so as to prevent leaks from the network elements.

2. A firewall system as recited in claim 1, wherein at least one of said front-end and back-end servers is configured to implement IP filtering.

3. A firewall system as recited in claim 2, wherein said front-end and back-end servers implement IP filtering according to the same rules.

4. A firewall system as recited in claim 1, wherein said back-end server is configured to capture at least one request from one of the network elements and to analyse said request for legitimacy before passing it to the public network.

5. A firewall system as recited in claim 1, wherein said back-end server is configured to detect a transfer of data from the network elements to the public network.

6. A firewall system as recited in claim 1, wherein at least one of said back-end internal and external interfaces and front-end internal and external interfaces is in the form of an ethernet card.

7. A firewall system as recited in claim 1, wherein said front-end server is configured with a first OS (Operating System) and said back-end server is configured with second OS.

8. A firewall system as recited in claim 7, wherein said first and second OS are different.

9. A firewall system as recited in claim 1, wherein said back-end server includes an application gateway.

10. A firewall system as recited in claim 1, wherein said back-end server includes a proxy service.

11. A firewall system as recited in claim 1, wherein said front-end server is so configured as to provide NAT (Network Address Translation).

12. A firewall system as recited in claim 11, wherein said NAT is so implemented as to not allow DNS (Domain Name System) to pass.

13. A firewall system as recited in claim 1, wherein said front-end server includes a third interface.

14. A firewall system as recited in claim 13, further comprising at least one of a DNS server, a web server, an email server and a time server connected to said third interface of the front-end server and wherein said third interface is configured so as to provide a DMZ (DiMilitarized Zone) for said at least one of a DNS server, a web server, an email server and a time server.

15. A firewall system as recited in claim 14, wherein said front-end server is configured to examine request sent to one of said at least one of DNS, web, email and time servers for potentially malicious commands.

16. A firewall system as recited in claim 13, further comprising a push mail server connected to said third interface of the front-end server and wherein said third interface is configured so as to provide a DMZ for said push mail server.

17. A firewall system as recited in claim 16, further comprising an internal email server connected to said internal interface of said back-end server; wherein said back-end server is configured to transfer email from said push mail server to said internal email server; whereby no email is allowed to pass through said front-end server directly to said back-end server.

18. A firewall system as recited in claim 16, wherein said push mail server is being configured to verify email for malicious content.

19. A firewall system as recited in claim 18, wherein said push mail server is configured to remove active content form emails.

20. A firewall system as recited in claim 18, wherein said push mail server is configured to scan emails for viruses.

21. A firewall system as recited in claim 17, further comprising an internal site firewall attached to said internal interface of said back-end server; said internal mail server being attached to said internal site firewall.

22. A firewall system as recited in claim 21, further comprising a DNS server attached to said internal site firewall.

23. A firewall system as recited in claim 21, further comprising a web server attached to said internal site firewall.

24. A firewall system as recited in claim 1, wherein said front-end server is attached to the public network via a router.

25. A firewall system as recited in claim 1, wherein said public network is the Internet.